Reliant™
REHABILITATION

Keep Information Safe with Good Password Practices

These days we're all overloaded with the number of accounts that require credentials and remembering them is impossible. Using the same password for different accounts is tempting—like having one handy key that opens every lock you use. But reusing passwords is not the solution.

Compromised passwords are one of the leading causes of data breaches, and reusing passwords can increase the damage done by what would otherwise be a relatively small incident. Cybercriminals know that people reuse credentials and often test compromised passwords on commonly used sites in order to expand the number of accounts they can access.

For instance, if you use the same password for your work email as for Amazon or your gym membership, a breach at one of those companies puts your work emails at risk. Reusing credentials is like giving away copies of the key that opens all your locks. Before reusing a password for different accounts, especially across work and personal ones, think of all the data that someone could get into if they got that credential.

Here are some tips to help you avoid falling in this trap:

- Use completely separate passwords for work and personal accounts.
- Avoid words that can easily be guessed by attackers, like "password" or "September2017," or predictable keyboard combinations like "1234567," "qwerty," or "1q2w3e4r5t."
- Add some complexity with capitalization or special characters if required. "Fido!sAnAwesomeDog" is a stronger password than your pet's name.
- Just adding numbers or special characters at the end of a word doesn't increase security much, because they're easy for software to guess.
- Avoid words like your kids' names that could easily be guessed by coworkers or revealed by a few minutes of online research.
- Answers to security questions are often easily found— your mother's maiden name is public record—so pick another word for whenever that question comes up.